Contoh Kasus Kriptografi di Kehidupan Nyata yang Terjadi Pada Tahun 2014 / 2015

Nama: A. F. Rashad

Kelas: SK7Pil

NIM: 09121001023

Penjelasan:

Kriptografi (atau kriptologi; dari bahasa Yunani κρυπτός *kryptós*, "tersembunyi, rahasia"; dan γράφειν *graphein*, "menulis", atau -λογία logi, "ilmu") merupakan keahlian dan ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga. Secara umum, kriptografi ialah mengenai mengkonstruksi dan menganalisis protokol komunikasi yang dapat memblokir lawan; berbagai aspek dalam keamanan informasi seperti data rahasia, integritas data, autentikasi, dan non-repudansi merupakan pusat dari kriptografi modern. Kriptografi modern terjadi karena terdapat titik temu antara disiplin ilmu matematika, ilmu komputer, dan teknik elektro. Aplikasi dari kriptografi termasuk ATM, password komputer, dan E-commerce.

Dalam menjaga kerahasiaan data dengan kriptografi, data sederhana yang dikirim (plainteks) diubah ke dalam bentuk data sandi (cipherteks), kemudian data sandi tersebut hanya dapat dikembalikan ke bentuk data sebenarnya hanya dengan menggunakan kunci (*key*) tertentu yang dimiliki oleh pihak yang sah saja. Tentunya hal ini menyebabkan pihak lain yang tidak memiliki kunci tersebut tidak akan dapat membaca data yang sebenarnya sehingga dengan kata lain data akan tetap terjaga.

Perdagangan elektronik (bahasa Inggris: electronic commerce atau e-commerce) adalah penyebaran, pembelian, penjualan, pemasaran barang dan jasa melalui sistem elektronik seperti internet atau televisi, www, atau jaringan komputer lainnya. E-commerce dapat melibatkan transfer dana elektronik, pertukaran data elektronik, sistem manajemen inventori otomatis, dan sistem pengumpulan data otomatis.

Industri teknologi informasi melihat kegiatan e-commerce ini sebagai aplikasi dan penerapan dari e-bisnis (e-business) yang berkaitan dengan transaksi komersial, seperti: transfer dana secara elektronik, SCM (supply chain management), pemasaran elektronik (e-marketing), atau pemasaran online (online marketing), pemrosesan transaksi online (online transaction processing), pertukaran data elektronik (electronic data interchange /EDI), dll.

E-commerce merupakan bagian dari e-business, di mana cakupan e-business lebih luas, tidak hanya sekedar perniagaan tetapi mencakup juga pengkolaborasian mitra bisnis, pelayanan nasabah, lowongan pekerjaan dll. Selain teknologi jaringan www, e-commerce juga memerlukan teknologi basisdata atau pangkalan data (databases), surat elektronik (e-mail), dan bentuk teknologi non komputer yang lain seperti halnya sistem pengiriman barang, dan alat pembayaran untuk e-dagang ini.

Kasus:

Menghindari penipuan pada transaksi online, Kementerian Komunikasi dan Informatika (Kemkominfo) mewacanakan situs e-commerce harus terakreditasi oleh suatu badan agar lebih terpercaya.

"Soal kasus Lazada tentang pengiriman iPhone 6 tersebut, harusnya bisa jadi momentum buat Kominfo percepat aturan e-commerce," jelas Menteri Komunikasi dan Informatika (Kominfo) Rudiantara di Jakarta.

Di Permen Kominfo, lanjut Rudiantara, perdagangan e-commerce perlu minta izin dari awal sehingga industri tersebut terpercaya di masyarakat.

"Tapi sebelum beroperasi harus tersertifikasi dan akreditasi, namun saya lebih senang akreditasi. Karena yang menyertifikat adalah Industri, untuk memastikan adanya perlindungan terhadap konsumen," tambahnya menjelaskan.

Dirinya juga menerangkan, Kemkominfo justru mendorong tumbuhnya e-commerce dan startup, registrasi secara administrasi serta mengajukan akreditasi ke badan untuk mendapatkan sertifikasi.

"Sertifikasi untuk menghadirkan kepercayaan kepada masyarakat sehingga ada certificate regulation self dari Industri, jadi lebih baik kita berdayakan iDea," tambah Rudiantara.

Sebelumnya, dunia maya dihebohkan dengan pemesanan iPhone 6 Plus melalui Lazada, namun yang diterima adalah sabun batangan. Ini dikicaukan akun @danisdarusman melalui jejaring sosial.

“Beli iphone 6+ nyampenya sabun nuvo! Hanya di @LazadaID BURUAN GUYS!!! Buruan bangkrut maksudnya lo,” kicau Danis di Twitter. Danis pun memposting foto boks pembungkus kiriman Lazada yang menunjukkan sabun batangan bukannya iPhone 6 Plus di dalamnya.

Sementara itu, pihak Lazada melalui Public Relation Manager-nya telah mengonfirmasi keluhan Danis Danuswara. Tania Amalia mengungkapkan jika pihaknya masih melakukan proses investigasi atas permasalahan tersebut.

Tania pun mengakui pihak Lazada telah langsung menghubungi pihak Danis Darusman selaku pelapor masalah.

“Sejauh ini kami masih melakukan proses investigasi, kami belum dapat menentukan pihak mana yang salah dalam kasus ini. Setelah investigasi selesai baru kami akan memberikan konfirmasi langsung terkait masalah itu,” ujar Tania melalui sambungan telefon.

Implementasi:

- ✓ Cara Kerja TCP/IP (tanpa SSL)

Kebanyakan transmisi pesan di internet dikirim sebagai kumpulan potongan pesan yang disebut paket. Pada sisi pengiriman, paket- paket dari sebuahpesan diberi nomor secara sekuensial. IP bertanggung jawab untuk merutekan paket (lintasan yang dilalui paket), dan setiap paket mungkin menempuh rute yang berbeda di dalam internet. Tujuan sebuah paet ditentukan oleh IP address, yaitu nomor yang digunakan untuk mengindentifikasi sebuah komputer pada sebuah jaringan.

Pada sisi penerima, TCP memastikan bahwa suatu paket sudah sampai, menyusunnya sesuai nomor urut, dan menentukan apakah paket tiba tanpa mengalami perubahan (misalnya berubah kasena physical error selama transmisi). Jika paket mengalami perubahan atau ada data yang hilang, TCP meminta pengiriman ulang. Bila semua paket dari pesan berhasil mancapai TCP/IP, pesan tersebut kemudian dilewatkan ke socket penerima. Socket tersebut menerjemahkan pesan kembali menjadi bentuk yang dibaca oleh aplikasi penerima (contoh aplikasi adalah HTTP, FTP, Telnet).

- ✓ Cara Kerja TCP/IP (menggunakan SSL)

Dari penjelasan sebelumnya dapat diketahui bahwa pada dasarnya TCP/IP tidak memiliki pengamanan komunikasi yang bagus. Bahkan, TCP tidak cukup canggih menentukan bilamana suatu paket berubah karena diubah oleh pihak ketiga (musuh), karena paket yang diubah tersebut dapat dianggap oleh TCP sebagai paket yang benar. Pada transaksi yang menggunakan SSL, SSL membangun hubungan (connection) yang aman antara dua socket, sehingga pengiriman pesan antara dua entitas dapat dijamin keamanannya.

SSL disusun oleh dua sub-protokol:

1. SSL handshaking, yaitu sub-protokol untuk membangun koneksi(kanal) yang aman untuk berkomunikasi.

2. SSL record, yaitu sub protokol yang menggunakan kanal yang sudah aman. SSL record membungkus seluruh data yang dikirim selama koneksi.

SSL mengimplementasikan kriptografi kunci public dengan menggunakan algoritma RSA dan sertifikat digital untuk mengotentikasi server di dalam transaksi san untuk melindungi informasi rahasia yang dikirim antara dua buah socket. Server selalu diotentikasi, sedangkan client tidak harus diotentikasi oleh server. Server diotentikasi agar client yakin bahwa ia mengakses situs web yang sah (dan bukan situs web palsu yang menyamar seolah-olah benar ia adalah server yang asli. Client tidak harus diotentikasi oleh server karena kebanyakan server menganggap nomor kartu kredit sudah cukup untuk mengotentikasi client.

Perlu dicatat bahwa SSL adalah protokol client-server, yang dalam hal ini web browser adalah client dan website adalah server. Client yang memulai komunikasi, sedangkan server memberi respon terhadap permintaan client. Protokol SSL tidak bekerja kalau tidak diaktifkan terlebih dahulu (biasanya dengan meng-klik tombol yang disediakan di dalam web server yang diakses oleh client.

1. Sub-protokol handshaking

Sub protokol handshaking diperlihatkan pada Gambar 4. Dari gambar tersebut terlihat bahwa SSL dimulai dengan pengiriman pesan Hello dari client ke server. Server merespon dengan mengirim pesan Hello dan sertifikat digital untuk otentikasi.

Sertifikat digital berisi kunci public server. Di dalam browser client terdapat daftar Certification Authority yang dipercaya. Jika sertifikat digital ditandatangani oleh salah satu Certification Authority di dalam daftar tersebut, maka client dapat memverifikasi kunci publik server. Setelah prose otentifikasi selesai, server mengirimkan pesan server done kepada client.

Selanjutnya, client dan server menyepakati session key untuk melanjutkan transaksi melalui proses yang disebut key exchange.

Session key adalah kunci rahasia yang digunakan selama transaksi. Nantinya, komunikasi antara client dan server dilakukan dengan menggunakan session key ini. Data yang akan ditransmisikan sienkripsi terlebih dahulu dengan session key melalui protokol TCP/IP. Proses key exchange diawali dengan client mengirim nilai acak 384-bit yang disebut premaster key kepada server. Nilai acak ini dikirim dalam bentuk terenkripsi (dienkripsi dengan kunci publik server). Melalui perhitungan yang cukup kompleks, client dan server menghitung session key yang diturunkan dari premaster key. Setelah pertukaran kunci, client dan server menyepakati algoritma enkripsi. SSL mendukung banyak algoritma enkripsi, antara lain DES, IDEA, RC2, dan RC4. Sedangkan untuk fungsi hash, SSL mendukung algoritma SHA dan MD5.

Gambar 1. Sub-protokol handshaking untuk membangun koneksi yang aman.

Client mengirim pesan bahwa ia sudah selesai mambangun sub-protokol. Server merespon client dengan mengirim pesan 8 dan 9 (change cipher dan finished). Sampai di sini, proses pembentukan kanal yang aman sudah selesai. Bila sub-protokol ini sudah terbentuk, maka http:// pada URL akan berubah menjadi https:// (http secure). Proses SSL yang cukup panjang ini menyebabkan sistem menjadi lambat. Oleh karena itu, SSL diaktifkan hanya bila client membutuhkan transmisi pesan yang benar- benar aman.

2. Sub-protokol SSL Record

Setelah kanal yang aman terbentuk, client dan server menggunakannya untuk menjalankan sub-protokol kedua (SSL Record) untuk saling berkirim pesan. Misalnya client mengirim HTTP request ke server, dan server menjawab dengan mengirim HTTP response.

Pesan dari client ke server (dan sebaliknya) dikirim dalam bentuk terenkripsi (pesan dienkripsi dengan menggunakan session key). Tetapi, sebelum pesan dikirim dengan TCP/IP, protokol SSL melakukan proses pembungkusan data sebagai berikut:

1. Pesan dipecah menjadi sejumlah blok (fragment) yang masing-masing panjangnya 16KB; setiap blok diberi nomor urut sekuensial.

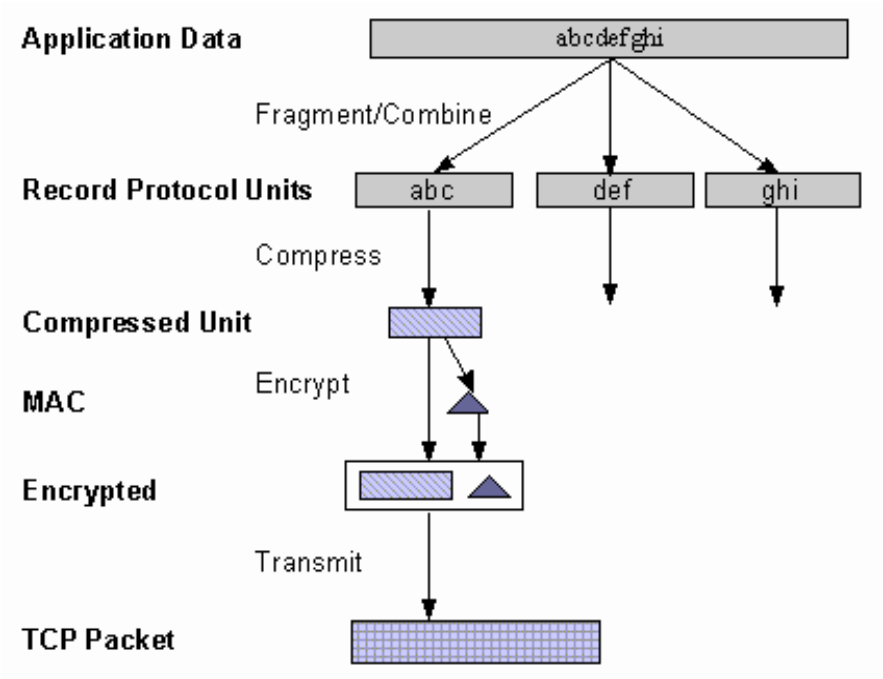
2. Setiap blok kemudian dikompresi, lalu hasil kompresi disambung (concate) dengan session key.

3. kemudian, hasil dari langkah 2 di atas di-hash dengan algoritma MD5 (atau algoritma hash lain yang disepakati). Nilai hash ini ditambahkan ke setiap blok sebagai MAC (Message Authentication Code). Jadi, MAC dihitung sebagai berikut:

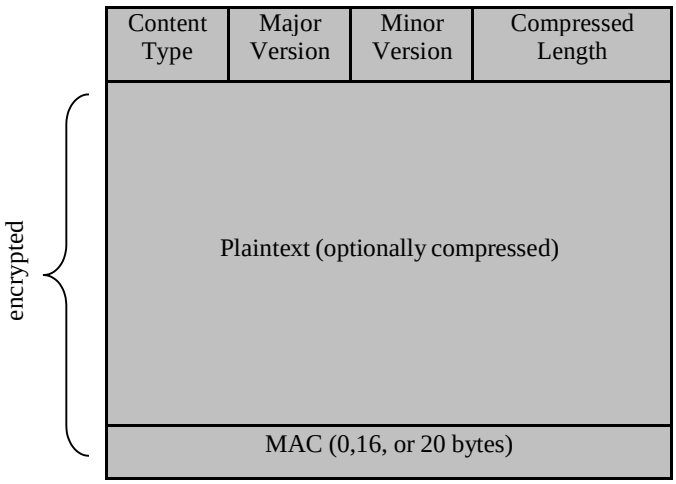
MAC = Hash (session key, compressed data block)

4. Hasil dari langkah 3 kemudian dienkripsi dengan algoritma kriptografi seimetri (misalnya RC4).

5. Terakhir, hasil dari langkah 4 diberi header (2 atau 3 byte), baru kemudian dikirim melalui koneksi TCP/IP aman yang terbentuk sebelumnya.



Gambar 2. Pembungkusan pesan oleh SSL Record



Gambar 3. Pembungkusan pesan oleh SSL Record

Proses pembungkusan pesan oleh sub-protokol SSL record diperlihatkan pada Gambar 2. Format SSL Record ditunjukkan pada Gambar 3. Setelah data sampai di tempat penerima, sub- protokol SSL ini melakukan proses berkebalikan: mendekripsi data yang diterima, mengotentikasinya (dengan MAC), mendekompresinya, lalu merakitnya.

Meskipun SSL melindungi informasi yang dikirim melalui internet, tetapi ia tidak melindungi informasi yang sudah disimpan di dalam server pedagang (merchant). Bila pedagang online menerima informasi kartu kredit atas pesanan suatu barang,, informasi tersebut mungkin didekripsi dan disimpan di dalam server pedagang sampai pesanan barang tersebut diantar. Jika server tidak aman dan data di dalamnya tidak dienkripsi, pihak yang tidak berhak dapat saja mengakses informasi rahasia tersebut.

Piranti keras, seperti kartu peripheral component interconnect (PCI) yang dirancang untuk digunakan di dalam transaksi SSSL, dapat dipasang ke dalam web server untuk memproses transaksi SSL, sehingga mengurangi waktu pemrosesan dan memungkinkan server bebas mengerjakan tugas-tugas lain.

Pada tahun 1996, Netscape Communications Corp. mengajukan SSL ke IETF (Internet Engineering Task Force) untuk standardisasi. Hasilnya adalah TLS (Transport Layer Security). TLS dijelaskan di dalam RFC2246. TLS dapat dianggap sebagai TLS versi 3.1, dan implementasi pertamanya adalah pada tahun 1999.

Wireless Transprt Layer Security (WTLS) adalah protokol keamanan data untuk Wireless Application Protocol. WAP adalah standar untuk komunikasi nirkabel (wireless) pada telepon mobile dan peralatan nirkabel lainnya. WTLS mengamankan kanal untuk komunikasi antara peralatan nirkabel dan server aplikasi.

Dengan fasilitas pertukaran data secara aman yang disediakan oleh SSL, teknologi ini banyak diadopsi oleh berbagai bisnis online di seluruh dunia.

Ada 3 metode dasar untuk membuat sbuah website E-Commerce yang aman menggunakan SSL:

1. Dengan membeli solusi SSL lengkap, termasuk sertifikat, dari vendor yang bonafid. Vendor-vendor ini menyediakan server yang telah dikonfigurasi secara penuh dan pemilik bisnis hanya tinggal membangun situs di atas server tersebut. Beberapa vendor menyediakan pula solusi Web- building.

2. Dengan membeli ”space” dari sebuah web-hosting di salah satu servernya yang elah mnyediakan fasilitas SSL. Ini disebut juga Co-Lo atau jasa hosting Co-Location. Perusahaan- perusahaan ini biasanya memiliki banyak server diberbagai lokasi dan memiliki koneksi internet yang cepat. Co-Lo dapat pula menangani registrasi domain dan mengurus sertifikat digital.

3. Dengan mambangun solusi sendiri. Di internet banyak Web Server open source dan aplikasi SSL yang tersedia secara gratis. Namun Sertifikat Digital masih harus dibeli secara terpisah.

Piranti-piranti yang dibutuhkan adalah sebagai berikut:

1. Sebuah server untuk difungsikan sebagai Web Server e-commerce.

2. Sebuah server redundant untuk difungsikan sebagai server mirror.

3. Firewall untuk melindungi jaringan internal.

4. Database server untuk menyimpan data untuk web server.

5. Backup device/server untuk menyimpan data backup dari database.

6. Cryptogaphic accelerator card, item opsional dan hanya dibutuhkan untuk menangani request halaman antara 300-500 halaman per detik pada web server. Karena SSL (dan TLS) memiliki fungsi kriptografis, berarti dibutuhkan kekuatan prosesor yang besar untuk menanganinya. Kartu ini dapat mengurangi beban kerja prosesor CPU dan meningkatkan kinerja web server.

Dengan melengkapi berbagai piranti di atas, server telah siap untuk menjalankan SSL. Namun, ada 3 hal lagi yang harus dipersiapkan agar SSL dapat berjalan, yaitu:

1. Sertifikat Digital SSL, dapat dibeli dari berbagai penyedia Sertifikat Digital (Certification Authority) terpercaya, seperti VeriSign, GTE CyberTrust, dan lain-lain.

2. Domain Name, salah satu syarat untuk mendapatkan Sertifikat Digital.

3. IP Address statis, syarat untuk mendapatkan Sertifikat Digital.

Sertifikat Digital tersedia dalam dua jenis, yaitu Sertifikat Digital private dan shared. Sertifikat Digital berjenis private hanya dijual ke perusahaan-perusahaan besar yang telah memiliki kredibilitas tinggi dengan domain name terkualifikasi dan IP address static. Sementara Sertifikat Digital berjenis shared ditujukan untuk perusahaan yang melakukan outsource dalam bisnisnya, seperti menitipkan server di Co-Lo.